

REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-19 are pending in this application, Claim 19 having been added. Support for added Claim 19 can be found, for example, in the original claims, drawings, and specification.¹ No new matter has been added.

In the outstanding Office Action, Claims 1-18 were rejected under 35 U.S.C. § 102(b) as anticipated by Akachi (U.S. Patent No. 7,069,436).

In response to the rejection of Claims 1-18 under 35 U.S.C. § 102(b) as anticipated by Akachi, Applicant respectfully requests reconsideration of the rejection and traverses the rejection as discussed next.

Independent Claim 1 is directed to a wireless ad-hoc communication system including, *inter alia*,

... a first terminal configured to encrypt a payload of a broadcast frame and to transmit the broadcast frame; and

a second terminal configured to receive the broadcast frame and to decode the payload of the broadcast frame,

wherein the first terminal is configured to encrypt the payload of the broadcast frame using a broadcast encryption key assigned to the first terminal, and

the second terminal is configured to decode the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal.

By way of background, Applicant's Claim 1 is directed to a wireless ad-hoc communication system in which the terminals are always moving. The terminals frequently

¹ See page 16, line 25 to page 17, line 12 and page 28 lines 12-19 of the specification; and in Figures 1 and 9.

participate in or are disconnected from a network, and therefore, terminals constituting a broadcast group cannot be fixed. In Claim 1, the first terminal (i.e. sending terminal) encrypts the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal, and the second terminal decodes the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal. In essence, this provides independent and distributed management of broadcast encryption keys, wherein the key neither need be common to several terminals nor be managed at one location.

In Akachi, the reception terminal decodes the packets using a common key which is common to a *plurality of reception terminals* as the decoding key for a broadcast,² rather than the broadcast encryption key assigned to the sending terminal, as in Applicant's Claim 1. Thus, an advantageous feature of a non-limiting embodiment of the Applicant's invention is that participants may join or leave the wireless communication system on an ad-hoc basis.

Accordingly, Applicant respectfully submits that the independent Claim 1 (and all claims depending thereon) patentably distinguishes over Akachi.

Independent Claim 4 recites, *inter alia*, a "means for searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of a *received broadcast frame* to extract the corresponding broadcast encryption key." Independent Claims 5 and 11 recite substantially similar features as independent Claim 4. Thus, the arguments presented below with respect to independent Claim 4 are applicable to independent Claims 5 and 11.

² See Akachi at column 8, lines 36-38.

Column 13, lines 36-44 of Akachi states that “when it is necessary to encrypt the data located in the payload, such as for an IP packet, the *transmission processing device 113* retrieves an encryption key assigned to the MAC address of the terminal 124i for arrangement within the section header. The encryption key is retrieved from the encryption key table stored in the encryption key table storage unit 113A and is used to encrypt an IP packet arranged in the payload of that section.” Thus, the process in Akachi is done in the *transmitter terminal*, and is not done in the *receiver terminal*.

Claim 2 recites a “means for decoding the payload of the broadcast frame *using the extracted broadcast encryption key assigned to the first terminal*,” and is also believed to be patentable for at least the reasons discussed above with regard to Claims 4, 5 and 11. Claim 2 is further believed to be patentable for the reasons discussed next.

Column 6, lines 47-52 of Akachi states that “the decoding unit 34 refers to a key table 37, *using the MAC address of the information processing device 22*, to obtain a decoding key from the key table 28. The decoding unit 34 then decodes the data stream D31 using the decoding key and supplies the resultant decoded data D34 to the checker 35.” The decoding key in Akachi is obtained according to the MAC address of the reception system. Thus, *the encryption key is not assigned to the first terminal* (i.e. transmission terminal), as in Claim 2.

Accordingly, Applicant respectfully submits that Claims 2, 4, 5, and 11 patentably distinguish over Akachi.

Claim 3 recites a terminal including, *inter alia*, “a generated-key table configured to store the broadcast encryption key assigned to the first terminal.” Independent Claims 6 and

7 recite substantially similar features as Claim 3. Thus, the arguments presented below with respect to Claim 3 are applicable to independent Claims 6 and 7.

Akachi describes that the encryption key table maintained in the transmission processing device 113 is for storing an encryption key table in the form of a diagram oriented to the encryption key assigned to *each MAC address*.³ In contrast, in Claim 3, the generated-key table of the terminal stores the encryption key of *the terminal itself*. Thus, Akachi fails to teach or suggest “a generated-key table configured to store the broadcast encryption key assigned to the first terminal,” as in Claim 3.

Accordingly, Applicant respectfully submits that Claims 3, 6, and 7 patentably distinguish over Akachi.

Independent Claim 8 recites a “means for encrypting a terminal identifier and a broadcast encryption key of the terminal using a unicast encryption key assigned to a transmission-destination terminal.” Independent Claim 9 recites substantially similar features as independent Claim 8. Thus, the arguments presented below with respect to independent Claim 8 are applicable to independent Claim 9.

Column 1, lines 24-29 of Akachi describes a *common key*, but does not describe a *unicast encryption key*. Thus, Akachi fails to teach or suggest the encryption of a broadcast encryption key using a unicast encryption key.

Accordingly, Applicant respectfully submits that the independent Claims 8 and 9 patentably distinguish over Akachi.

³ See Akachi at column 13 lines 16-19.

Independent Claim 12 recites a method for “encrypting a broadcast frame in a terminal that includes a generated-key table storing a broadcast encryption key assigned to said terminal.” Independent Claim 16 recites substantially similar features as independent Claim 12. Thus, the arguments presented below with respect to independent Claim 12 are applicable to independent Claim 16.

As discussed above with regard to Claims 3, 6, and 7, Akachi fails to teach or suggest encrypting a broadcast frame in a terminal that includes “a generated-key table storing a broadcast encryption key of said terminal.”

Accordingly, Applicant respectfully submits that the independent Claims 12 and 16 also patentably distinguish over Akachi.

Independent Claim 13 recites a “receiving a terminal identifier and a broadcast encryption key that are encrypted *using a unicast encryption key between the first terminal and the second terminal*” and “decoding . . . *using the unicast encryption key;*” and “encrypting a terminal identifier . . . *using the unicast encryption key.*” Independent Claims 14, 17, and 18 recite substantially similar features as independent Claim 13. Thus, the arguments presented below with respect to independent Claim 13 are applicable to independent Claims 14, 17, and 18.

In contrast, column 1, lines 24-29 of Akachi describes encryption by a common key and fails to teach or suggest the use of a unicast encryption key to encode the common key.

Accordingly, Applicant respectfully submits that the independent Claims 13, 14, 17, and 18 patentably distinguish over Akachi.

Independent Claim 10 recites a “means for encrypting the terminal identifier and the broadcast encryption key of the different terminal using a broadcast encryption key assigned to the terminal,” and is thus believed to be patentable for at least the reasons discussed above with regard to independent Claims 14 and 18.

Claim 10 is further believed to be patentable for at least the reasons discussed next. Column 1, lines 24-29 of Akachi describes encryption using a common key and fails to teach or suggest using the broadcast key of a receiving terminal to encrypt or encode the broadcast key of the transmitting terminal.

Accordingly, Applicant respectfully submits that the independent Claims 10, 14, and 18 patentably distinguish over Akachi.

Thus, Applicants respectfully request that the rejection under 35 U.S.C. § 102(b) as anticipated by Akachi be withdrawn.


In order to vary the scope of claim coverage, new Claim 19 has been added. New Claim 19 finds non-limiting support in the disclosure as originally filed, for example, at page 16, line 25 to page 17, line 12; page 28 lines 12-19; and in Figures 1 and 9. Therefore, the changes to the claims are not believed to raise a question of new matter.⁴

⁴ See MPEP 2163.06 stating that "information contained in any one of the specification, claims or drawings of the application as filed may be added to any other part of the application without introducing new matter."

Consequently, in view of the present amendment, and in light of the above discussion, the pending claims as presented herewith are believed to be in condition for formal allowance, and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Derek P. Benke
Registration No. 56,944